KPMG

Circular 2017/1 Corporate Governance – Banks

Corporate governance, risk management and internal controls at banks

FINANCIAL SERVICES

Circular 2017/1 Corporate Governance – Banks

Corporate governance, risk management and internal controls at banks

Other languages:

FR: Gouvernance d'entreprise - banques (31.10.2019)

IT : Corporate governance - banche (31.10.2019)

Unofficial translation of September 2019

Circular 2017/1
Corporate Governance – Banks

Corporate governance, risk management and internal controls at banks

Reference:	FINMA circ. 17/1 "Corporate Governance – Banks"
Issued:	22 September 2016
Entry into force:	1 July 2017
Last amendment:	31 October 2019 [amendments are denoted with an * and are listed at the end of the document]
Concordance:	previously FINMA circ. 08/24 "Supervision and Internal Control – Banks" dated 20 November 2008
Legal bases:	FINMASA Article 7(1)(b) BA Articles 3(2)(a) and (c), 3b–3f, 4^{quinquies}, 6 BO Articles 11(2), 12 SESTA Articles 10(2)(a) and (5), 14 SESTO Articles 19, 20 CAO Articles 7–12

Addressees

BA			ISA			SESTA	FMIA						CISA									AMLA			OTHERS	
Banks	Financial groups and congl.	Other intermediaries	Insurance companies	Ins. groups and congl.	Distributors	Securities dealers	Trading Venues	Central Counterparties	Central depositories	Trade repositories	Payment systems	Participants	Fund management companies	SICAV	Limited partnerships for CIS	SICAF	Custodian banks	Managers domestic CIS	Distributors	Representatives of foreign CISs	Other intermediaries	SROs	DSFIs	SRO Supervised	Audit firms	Rating Agencies
X	X					X																				

Table of Content

I. Subject matter

The present circular shall set out the requirements in regard to corporate governance, risk management, the internal control system (ICS) and the internal audit at banks, securities dealers, financial groups (Article 3c(1) BA) and financial conglomerates dominated by banks or securities dealers (Article 3c(2) BA). In the following, these shall be referred to as institutions. 1

II. Terms

In the following, corporate governance shall mean the principles and structures with which the bodies of the institution manage and control it. 2

Risk management shall comprise the organizational structures as well as the methods and processes used to determine risk strategies and risk management measures, as well as to identify, analyze, measure, manage, monitor and report risks. 3

Risk appetite shall include both quantitative and qualitative considerations on material risks that the institution is willing to enter into in order to achieve its strategic business objectives considering its capital and liquidity planning. Risk appetite shall be defined for each risk category as well as at the level of the institution, if this is relevant. 4

The risk profile shall provide an overall picture, at the level of the institution and for each risk category and for a specific point in time, the risk exposure that the institution has assumed. 5

The ICS shall encompass the entire controlling structures and processes that allow the institution to achieve its business objectives on all levels, ensuring orderly business operations. The ICS does not only contain retroactive activities but shall also contain planning and management elements. An effective ICS shall consist of control activities integrated into the work processes, appropriate risk management and compliance processes, as well as control instances appropriately designed for the institution's size, complexity and risk profile, especially an independent risk control and compliance function. 6

Compliance shall be understood as the adherence to legal, regulatory and internal regulations, as well as abiding by common market standards and rules of professional conduct. 7

III. Scope (principle of proportionality)

This circular shall apply to all institutions defined in margin number 1. The requirements shall be implemented on a case-by-case basis, taking into account the relevant institution's size, complexity, structure and risk profile. In individual cases, FINMA may grant simplifications or set tighter requirements. 8

IV. Governing body

A. Duties and responsibilities

The duties of the governing body for the guidance, supervision and control, hereinafter "governing body", shall specifically encompass: 9

a) Business strategy and risk policy

The governing body shall define the business strategy and shall define the guiding principles for the institution's corporate culture. It shall approve a risk policy as well as the framework concept for the institution-wide risk management and bear responsibility for establishing, regulating, and monitoring an effective risk management as well as managing overall risks. 10 *

b) Organization

The governing body shall be responsible for an adequate business organization and shall issue the necessary policies for this. 11

c) Finances

The governing body shall bear the ultimate responsibility for the institution's financial situation and its development. It shall approve the capital and liquidity planning as well as the annual report, the annual budget, the interim financial statements and the annual financial objectives. 12

d) Staff and other resources

The governing body shall be responsible for ensuring that the institution possesses adequate staff and other resources (e.g. infrastructure, IT) as well as HR and remuneration policies. It shall appoint and remove from office of the members of its committees, the members of the executive board, the CEO, the Chief Risk Officer (CRO) as well as he Head of Internal Audit[1]. 13

The governing body shall exercise ultimate oversight over the executive board. It shall ensure an appropriate risk control environment within the institution, establish an effective internal control system, appoint and supervise the internal auditors, appoint the regulatory auditors, and evaluate audit reports. 14

e) Major changes in the corporate structure and investments

The governing body shall decide on major changes to the corporate or group structure, major changes at significant subsidiaries and other projects of strategic significance. 15

[1] The Head of Internal Audit may also be selected by the audit committee.

B. Members of the governing body

a) General requirements

In its entirety, the governing body shall dispose of sufficient leadership competence and the necessary expertise and experience in the banking and financial service sector. It shall be sufficiently diversified to ensure the competent representation of all of the main business areas, such as accounting and finance as well as risk management. 16

b) Independence

At least a third of the members of the governing body shall be independent. Should this be justified, such as in the case of purely domestic financial groups, the FINMA may grant exceptions. 17

A member of the governing body shall be deemed independent if he or she: 18

- is not employed in any other function at the institution and has not been so in the last 2 years; 19
- has not been employed as the responsible lead auditor with the audit company of the institution within the last 2 years; 20
- does not maintain business relationships with the institution which, in view of their type or scope, may lead to a conflict of interests; and 21
- is not a qualified shareholder according to Article 3(2)(c^{bis}) BA and Article 10(2)(d) SESTA, and also does not represent such a person. 22

Members appointed to or elected to a governing body of a cantonal or municipal bank by cantons, communities or other cantonal or municipal institutions shall be deemed to be independent according to margin no. 18-22, if they: 23

- are neither part of the cantonal or municipal government or administration nor belong to any other cantonal or municipal company under public law, and 24
- do not receive any instructions from their appointing body for their activity as a member of the governing body. 25

C. Basic principles governing a directorship

Every member of the governing body shall devote a sufficient amount of time to his or her mandate and play an active role in the strategic management and oversight of the company. He or she shall perform the mandate in person and be available beyond the normal meeting schedule in the event of crises or emergencies. 26

The governing body shall determine the required qualifications profile for its members, chair and committee members as well as for the CEO. It shall approve and regularly assess the qualifications profiles of the remaining members of the executive board, the CRO and the Head of Internal Audit. It shall ensure appropriate succession planning. 27

At least once a year, the governing body shall critically assess its own performance (including its achievement of objectives and its working methods), with the aid of a third party if necessary, and keep a written record of the results. 28

The governing body shall regulate how to approach conflicts of interests. Current and former interests shall be disclosed. If a conflict of interests cannot be avoided, the institution shall take the appropriate measures to mitigate or eliminate these. 29

A. Segregation of duties and committees

a) Role of the chairperson

The chairperson shall preside over the entire body and act as internal and external representative for the governing body. He/she shall hold a key role in shaping the company's strategy, communication and corporate culture. 30

b) Committees

Institutions in supervisory categories 1 - 3 shall establish a separate audit committee and risk committee. Institutions in supervisory category 3 may combine their audit and risk committees. Systemically important institutions shall have a nomination committee and remuneration committee at least at group level. The committees shall ensure appropriate reporting to the overall governing body. 31

The audit committee shall make sure that it differs sufficiently from the other committees in terms of its personnel composition. 32

As a rule, the majority of the members of the audit and risk committees shall be independent (cf. margin nos. 18 - 25). 33

In principle, the chairperson of the governing body may not be a member of the audit committee or the chair of the risk committee. In their entirety, the committees shall have sufficient knowledge and experience in the area of the relevant committee.

c) Duties of the audit committee

In particular, the duties shall encompass the: 34

- preparation of the general guidelines for the internal audit function and the financial reporting to the attention of the governing body; 35
- monitoring and assessment of the financial reporting and the integrity of financial statements, including a discussion of these with the member of the executive board responsible for finance and controlling, the external leading auditor, and Head of Internal Auditor; 36
- monitoring and assessment of the effectiveness of the internal controls, specifically those related to risk control, compliance and internal audit, unless this duty has already been assumed by the risk committee; 37

- monitoring and assessment of the effectiveness and independence of the external auditor as well as its coordination with Internal Audit, including the discussion of the audit reports with the external leading auditor; 38

- appraisal of the audit plan, the audit frequency and the audit results of Internal Audit and the audit firm. 39

d) Duties of the risk committee

In particular, the duties shall encompass the: 40

- discussion of the risk policy and the framework concept for the institution-wide risk management as well as the recommendations to the entire governing body; 41*

- evaluation of the capital and liquidity planning and the relevant reporting to the entire governing body; 42

- at least an annual assessment of the institution's risk policy and the framework concept of the institution-wide risk management, ensuring the necessary changes are made; 43*

- review of whether the institution maintains an adequate risk management with effective processes that are in line with the institution's risk situation; 44

- monitoring of the implementation of risk strategies, especially in regard to their alignment with the pre-defined risk appetite as well as the risk limits in accordance with the risk policy and the framework concept of the institution-wide risk management. 45*

The risk committee shall regularly receive from the Chief Risk Officer (CRO) and other relevant function holders meaningful reports on the relevant aspects of the framework concept for the institution-wide risk management (as per margin nos. 52 - 59) and compliance with it. 46*

V. Executive board

A. Duties and responsibilities

The executive board shall be responsible for the operational activities in line with the business strategy, the instructions and decisions made by the governing body. It is specifically responsible for the: 47

- management of day-to-day business as well as operating income and operational risk management, including the management of the balance sheet structure and liquidity as well as the representation of the institution towards third parties in operational matters; 48

- submission of proposals in respect of matters that fall under the responsibility of (or are potentially subject to) the approval of the governing body and the formulation of policies regulating the operating activities; 49

- design and maintenance of internal processes fit for purpose, an adequate management information system (MIS), an internal control system (ICS) as well as an appropriate technological infrastructure. 50

B. Requirements to be met by members of the executive board

As a collective body and as persons responsible for leadership, members of the executive board shall have sufficient management competence as well as the necessary expertise and experience in banking and finance to adequately ensure the adherence to the licensing requirements within the scope of operational activities. 51

VI. Risk policy and institution-wide risk management framework

The framework concept for the institution-wide risk management shall be formulated by the executive board, approved by the governing body and documented appropriately. 52*

The risk policy and the framework concept for the institution-wide risk management shall regulate the management of key risks, the risk appetite and the risk limits for all significant risk categories based on these. 53*

Institutions in supervisory categories 1-3 shall in particular take into consideration the following aspects: 54*

- Standardized categorization[2] of the key risks in order to ensure consistency in the setting of objectives in risk management; 55
- Specification of the possible losses from these significant risk categories; Definition and use of tools as well as organizational setup to identify, analyze, value, manage, monitor significant risk categories and the reporting; 56
- Identification, analysis, valuation, management, monitoring of significant risk categories and reporting; 57
- Design of a documentation that enables an adequate review of the definition of the risk appetite as well as the relevant risk limits; 58
- Definition of the risk data aggregation and reporting at institutions in supervisory categories 1-3. In the case of systemically important institutions, these definitions shall specifically contain information on the data architecture and IT infrastructure that allow for an aggregated and timely risk analysis and valuation as well as a risk data aggregation and reporting for all of the institution's significant risk categories under normal conditions as well as in periods of stress. 59

[2] Depending on the nature, type and level as well as using the regulatory definitions given in the CAO.

VII. Internal control system

There shall be at least two controlling bodies within the ICS: the revenue-generating business units and the control bodies, which are independent of them. 60

A. Revenue-generating business units

Revenue-generating business units shall carry out their control function as part of their daily activities by managing risks and specifically by directly monitoring, managing and reporting on them. 61

B. Independent control bodies

The independent control body shall monitor the risks as well as the adherence to laws, regulations and internal policies. Individual institutions may establish a variety of control bodies which must, however, at least cover the duties and responsibilities of risk control (margin nos. 69–76) and the compliance function (margin nos. 77–81). 62

The compensation system for independent control bodies shall not set any incentives that could lead to conflicts of interests with the tasks of these bodies. 63

a) Establishment and reporting line

Within the scope of their tasks, the independent control bodies shall have unrestricted information, access, and inspection rights, and must be integrated into the overall organization and internal control system independently of the revenue-generating business units. The independent control bodies shall be equipped with appropriate resources and competencies. 64

The institution shall define one or several persons on the executive board who are responsible for the independent control bodies. 65

The institution shall ensure that such independent control bodies have direct access to the governing body. 66

Institutions in supervisory categories 1-3 shall appoint independent risk control and compliance functions that act as independent control bodies. They shall appoint a CRO who may be responsible for risk control as well as other independent control bodies. 67

Systemically important Institutions shall appoint a CRO who is part of the executive board. Duties and responsibilities of risk control 68

Risk control shall be responsible for ensuring the systematic monitoring and reporting of both individual and aggregated risk exposures. As part of quantitative and qualitative analyses, this shall include the conducting of stress tests and scenario analyses under unfavorable business conditions. Institutions subject to the small banks regime pursuant to Articles 47a-47e CAO shall have to conduct at least scenario analyses. 69*

In institutions in supervisory categories 1-3, risk control shall also ensure the adequate implementation of 70

the provisions on risk data aggregation and reporting as set out in margin no. 59.

In particular, risk control shall monitor the institution's risk profile to determine that it is in line with the risk appetite and the risk limits defined in the risk policy and the framework concept for the institution-wide risk management. 71*

Risk control shall also be responsible for the design and the operation of adequate risk monitoring systems, the definition and implementation of principles and methods for the risk analysis and valuation (e.g. valuation and aggregation methods, validation of models) as well as the monitoring of systems to ensure that these comply with regulatory provisions (especially in regulations relating to capital adequacy, risk diversification and liquidity). 72

Risk control shall be appropriately consulted in the development of new or expanded product categories, services, business areas or markets, as well as in major or complex transactions. 73

Risk control shall actively participate in the definition of risk limits and shall specifically ensure that risk limits are in line with the institution's risk appetite and that they match the results of the stress tests and that they are defined in such a way that they are an operationally effective management tool for the executive board. 74

Risk control shall report to the executive board on the development of the institution's risk profile as well as its activities as per margin nos. 69-78 at least every 6 months and to the governing body at least annually. A copy of these reports shall be provided to Internal Audit and the audit firm. 75

Risk control shall inform the executive board and internal Audit in a timely manner of special developments and in the case of matters with far-reaching implications, also the governing body. 76

b) Duties and responsibilities of the compliance function

At a minimum, the duties and responsibilities of the compliance function shall encompass the following activities: 77

- annually, assess the compliance risks of the institution's business activity and prepare a risk-oriented activity plan to be signed off by the executive board. This activity plan must also be made available to Internal Audit; 78
- report to the executive board on significant changes in the assessment of the compliance risk in a timely manner; 79
- annually report to the executive board its assessment of compliance risks and report on the activities of the compliance function. A copy of these reports shall be provided to Internal Audit as well as the audit firm; 80
- report to the executive board and the governing body on any serious compliance breaches or matters with far-reaching implications in a timely manner, as well as support the executive board in its choice of instructions and measures to be taken. Internal Audit shall be informed accordingly. 81

VIII. Internal Audit

A. Establishment

As a rule, every institution shall establish an internal audit function. 82

Should the establishment of an institution-specific Internal Audit function be deemed disproportionate, internal auditing duties may be delegated to: 83

- Internal Audit of the parent company or of another group company, provided this company is also a bank, a securities trader or another state-supervised financial intermediary (e.g. insurance company) (for foreign banks, Article 4quinquies BA shall apply); 84
- a second external audit firm that is independent of the institution's regulatory audit firm; or 85
- a group company or an independent third party, provided the audit firm confirms their professional competence and the adequacy of their technical resources and staffing. 86

B. Reporting line and organization

Internal Audit shall report to the governing body or its audit committee, and fulfill the auditing and monitoring tasks assigned to it independently. It shall be accorded unlimited rights to inspect, receive information and audit within the institution and all of its companies subject to consolidation pursuant to margin no. 98. 87

Internal Audit shall be designed in line with the size, complexity and risk profile of the institution; it forms an autonomous organizational unit that is independent of business operations. 88

Internal Audit shall meet the quality standards promulgated by the Swiss Institute of Internal Auditing (IIA). Internal Audit shall follow the international Standards for the Professional Practice of Internal Auditing of the Institute of Internal Auditors (IIA). 89

The system of remuneration for Internal Audit employees may not contain any incentives which could lead to conflicts of interests. 90

C. Duties and responsibilities

Internal Audit shall deliver independent audits and assessments on the adequacy and effectiveness of the corporate organization and business processes, especially on the institution's internal control system and risk management. 91

Internal Audit shall conduct a comprehensive risk assessment of material risk categories of the institution in accordance with margin no. 53 at least once a year, thereby considering external developments (e.g. economic environment, regulatory changes) and internal factors (e.g. important projects, business focus) in an adequate manner. Internal audit functions of institutions subject to the small banks regime (Articles 47a-46e CAO) may conduct this assessment every two years, provided the institution's risk profile has not changed significantly. 92*

Basing itself on this risk assessment and any other audit requirements that might arise, Internal Audit shall define the audit objectives and audit planning for the next audit period; material changes shall be approved by the governing body or its audit committee. 93

Internal Audit shall make sure the executive board and the audit firm are informed of the risk assessment and the audit objectives. 94

Internal Audit shall prepare a written report on the key audit findings of its audits in a timely manner, and submit this report to the governing body or its audit committee. 95

Internal Audit shall prepare a written report at least once a year which contains the significant audit results and the key activities of the audit period; it shall submit this report and the relevant conclusions to the governing body or its audit committee, the executive board and the audit firm for their consideration. 96

Furthermore, Internal Audit or another independent unit within the institution (such as the compliance function or risk control) shall inform the governing body or the audit committee at least every six months of the remediation of any identified major shortcomings and the status of implementation of any recommendations made by Internal Audit and the audit firm. 97

IX. Group structures

By extension, the principles and provisions of this Circular shall also apply to financial groups and conglomerates ("groups"). 98

Groups shall regulate duties and responsibilities of units that hold an overall responsibility for the group's management. The standards defined shall ensure the efficient and uniform management of the group, permit the appropriate exchange of information, take into account the legal and organizational structures and define the duties and responsibilities and the necessary independence of the respective management levels, taking into account the business activities and material risks at group and individual institution level. Particular attention shall be paid to risks that arise from the merger of several companies to form a single commercial entity. 99

X. Transitional provisions

Repealed 100*-104*

For systemically important banks, the expanded provisions on the risk data aggregation and reporting (margin no. 59) the later of the dates mentioned in the following below shall apply: 105

- entry into force of this circular; or
- a three-year-long transitional period applicable after a bank has been designated as a systemically important bank pursuant to Article 8(3) BA.

List of amendments

The circular has been amended as follows:

These amendments were passed on 31 October 2019 and entered into force on 1 January 2020.

Amended margin nos.	10, 41, 43, 45, 46, 52, 53, 54, 69, 71, 92
Repealed margin nos.	100, 101, 102,103, 104
Other amendments	New title before margin no. 52

Contacts

Philipp Rickert
Partner, Head of Financial Services,
Member of the Executive Committee
Zurich
Tel. +41 58 249 42 13
prickert@kpmg.com

Helen Campbell
Partner, FS Transformation
Tel. +41 58 249 35 01
hcampbell@kpmg.com

Thomas Dorst
Partner, Assurance & Regulation
Tel. + 41 58 249 54 44
tdorst@kpmg.com

Nicolas Moser
Partner, Geneva Office
Tel. +41 58 249 37 87
nmoser@kpmg.com

www.kpmg.ch